Notice of Allowability	Application No.	Applicant(s)	
	09/490,354	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *01/19/06 and interview agreement on 02/07/06*.

2. ☒ The allowed claim(s) is/are *1-1-24, 26-29, 33-38, 40-45 and 49-55 now, re-numbered as claims 1-47*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

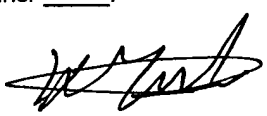
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *enclosed* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.



DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Arik B. Ranson on 02/06/2006.

The application has been amended as follows:

Claim 1

(Currently Amended) A computerized method for delivering a digital ticket from a ticket provider to a ticket consumer across a communications channel, the method comprising:

first communicating, across a communications channel from a computer of a ticket provider to a computer of the ticket consumer, first digital data D_1 in respect of an occurrence relating to the ticket; and

second communicating, across the communications channel from the computer of the ticket consumer to the computer of the ticket provider, second digital data D_2 relating to purchase of the ticket; and

calculating in the computer of the ticket provider by use of a private key s a digital signature of third digital data D_3, which third digital data D_3 is in respect of one or both of the first digital data D_1 and the second digital data D_2, and which digital signature of the digital data D_3 is as well, being a proof both (i) that a private signature key s was used by the computer of the ticket provider in generation of the digital signature and (ii) that one or both of the digital data D_1, D_2 was used in respect of its generation, (iii) suitably stored in a transportable storage medium; and

wherein the digital data D_1, D_2 in respect of which the digital signature of digital data D_3 was generated becomes a memorialization of a particular provision by the ticket provider of the particular digital ticket for the particular occurrence to the ticket consumer who is particularly identified at least as a party at the other end of the communicating transpiring across the communications channel; and

third communicating, across the communications channel from the computer of the ticket provider to the computer of the ticket consumer, at least the signed digital data D_3; and

first storing with the computer of the ticket consumer in the transportable storage medium at least the signed digital data D_3, thus turning the transportable storage medium into a digital ticket; and

physically transporting the digital ticket in the form of the transportable storage medium so containing at least the signed digital data D_3, to a specific place for the occurrence relating to the ticket; and

tendering the digital ticket for redemption to a ticket taker at the specific place; and

reading into a computer of the ticket taker at least the signed digital data D_3; and

recovering in the computer of the ticket taker, with a digital verification key *v* corresponding to the signature key s of the ticket provider and from the signed digital data D_3, the digital data D_3; and

determining in the computer of the ticket taker IF the digital data D_3 was recoverable by verification key *v* AND, having been so recovered, the digital data D_3 correctly memorializes the particular provision by the ticket provider of the particular third digital data D_3 for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is valid, ELSE IF the digital data D_3 was recovered by use of the verification key *v* BUT the digital data D_3 recovered incorrectly memorializes the particular provision by the ticket provider of the particular third digital data D_3 for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is invalid; wherein the second communicating is of second digital data D_2 including a one-way function hash (R) of a number R which number R is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider.

Claim 2

(Currently Amended) The digital ticket computerized delivery and redemption method according to claim 1 [wherein the second communicating is of second digital data D_2 including a one-way function hash (R) of a number R which number R is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider;] wherein the calculating in the computer of the ticket provider is of a digital signature in respect of the third digital data D_3 including the one way function of hash (R) plus information I concerning the event for which the ticket is had, Sign (s, I | | hash (R));

wherein the third communicating is of Sign (s, I | | hash (R));

wherein the first storing is of R appended to Sign (s, I | | hash (R)), or Sign (s, I | | hash (R)) | | R, as the digital ticket;

wherein the reading into the computer of the ticket taker is of the Sign (s, I | | hash (R)) | | R;

wherein the recovering in the computer of the ticket taker of the I | | hash (R) gives hash (R); and, having both R and hash (R) to hand,

wherein the determining further proceeds by recalculating the hash (R) in respect of R, so that IF the recalculated hash (R) equals to the recovered hash (R) of the digital ticket as read THEN the digital ticket is valid ELSE IF the hash (R) does not equal to the recovered hash (R) of the digital ticket as read THEN the digital ticket is invalid.

Claim 30

(Cancelled)

Claim 32

(Cancelled)

Claim 34

(Currently Amended) A digital ticket comprising:

a tangible transportable digital data storage medium containing

first-type data, originally known both to a buyer and to a seller of a ticket and meaningful to at least the seller of the ticket to identify, at least relatively, a particular event for which the ticket was sold, and

second-type data including a signed digital representation of a particular parameter that was originally computer-generated in a sequence first by the buyer of the ticket as a non-invertible function of a random number called a "first-time-made non-invertible function", wherein the non-invertible function is a one-way hash function, and wherein the random number is uniquely known to the buyer and not to the seller, and then

second by the seller of the ticket as a digital signature of the first-time-made non-invertible function, and then

third by the buyer of the ticket to attach the selfsame random number;

wherein, to validate the digital ticket upon attempted redemption of the ticket, the random number is detached, and then

the signed first-time-made non-invertible function is interpreted, recovering this first-time-made non-invertible function, and then

the non-invertible function of that selfsame random number just detached is newly made all over again, which newly made non-invertible function is called the "second-time-made non-invertible function";

wherein the second-time-made non-invertible function EITHER equals the first-time-made non-invertible function IN WHICH CASE the ticket is not invalid OR ELSE the second-time-made non-invertible function does not equal the first-time-made non-invertible functional thus making the digital ticket is invalid for at least the particular event.

Claim 38

(Currently Amended) A system for delivering a digital ticket from a ticket seller to a ticket buyer, the system comprising:

a communication channel comprising means for, at a first time, sending from a ticket seller to a ticket buyer data regarding events for which tickets may be had, means for, at a second time, sending from the ticket buyer to the ticket seller data representative of a non-invertible transformation of a number determined by the ticket buyer only, and means for, at a third time, sending from the ticket seller to the ticket buyer a digital signature of the non-invertible transformation, wherein the received digital signature of the non-invertible transformation is combined with the number to produce a digital ticket;

a ticket buyer's computer, communicatively connected to the communications channel, the ticket buyer's computer comprising means for determining the number, means for computing the non-invertible transformation, and means for combining the digital signature of the non-invertible transformation with the number to produce a digital ticket;

a ticket seller's computer, communicatively connected to the communications channel, the ticket seller's computer comprising means for computing, in respect of the non-invertible transformation received from the ticket buyer, the digital signature of the non-invertible transformation; and

a tangible portable medium of digital data storage connected to the buyer's computer and storing the digital ticket;

wherein the communication channel is sending at the second time a random number.

Claim 39

(Cancelled)

Claim 45

(Currently Amended) A printed ticket bearing indicia CHARACTERIZED IN THAT the indicia includes a 2-D bar code containing a one-way function of a number provided by a holder of the ticket, the one-way function being digitally signed by a provider of the ticket;

FURTHER CHARACTERIZED IN THAT the 2-D bar coded indicia contains Sign (s, I | | hash (R)) | | R where

(1) R is a number having its origin in a computer of a consumer of the ticket, which number R is appended to

(2) a number Sign (s, I | | hash (R)) that was computed in a computer of a provider of the ticket as a digital signature in respect of digital signature key s of the number hash (R) in combination with information I,

subsequently communicated across the communications network to the computer of the ticket consumer, which number hash (R) was itself computed in the computer of the ticket provider as a one way function of R and subsequently communicated to the computer of the ticket provider;

wherein number R, having its origin in a computer of the ticket consumer, is private to the ticket consumer and is not public; and

wherein the digital signature key s of the computer of the ticket provider is private to the ticket provider and is not public.

Claim 48

(Cancelled)

Claim 49

(Currently Amended) A communications system for selling and delivering a digital ticket comprising:

a ticket buyer computer (i) sending at a first time a one-way transformation of a private number to a seller computer, (ii) receiving at a third time signed information from the ticket seller computer, and (iii) storing at a fourth time within a digital store the received encrypted signed information plus the private number;

a ticket seller computer (i) receiving at the first time the one-way transformation of the private number from the seller computer, (ii) signing at a second time this one-way transformation and additional information, and (iii) sending at the third time the signed first transformation and additional information to the ticket buyer computer as signed information; and

a digital store storing at the fourth time the signed information plus the private number as a digital ticket;

wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing with the same secure first transformation that the ticket seller used the secure first transformation of the number all over again, and (iv) a comparing of the decrypted recovered one-way transformation to the reproduced first transformation, validity of the digital ticket is assessable;

wherein the second communicating is of second digital data D_2 including a one-way function hash (R) of a number R which number R is uniquely known to the computer of the ticket buyer and not to the computer of the ticket seller.

Claim 50

(Currently Amended) A method for selling and delivering a digital ticket comprising:

first-sending at a first time a one-way transformation of a private number from a ticket buyer computer to a ticket seller computer, wherein the private number is a random number; first-receiving at the first time the one-way transformation of the private number in the ticket seller computer;

signing at a second time the one-way transformation and additional information in the ticket seller computer;

second-sending at a third time the signed first transformation and additional information as signed information from the ticket seller computer to the ticket buyer computer;

second-receiving at the third time the signed information in the ticket buyer computer;

storing with the ticket buyer computer at a fourth time both (i) the received signed information plus (ii) the private number within a digital memory store;

storing within the digital memory store at the fourth time the signed information plus the private number as s digital ticket;

wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing, with the same secure first transformation that the ticket seller used, the secure first transformation of the number all over again, and (iii) a comparing of the decrypted recovered one-way transformation to the reproduced first transformation, validity of the digital ticket is assessable.

Claim 51

(Currently Amended) In a communications system having a computer of a ticket buyer bi-directionally communicating across an insecure digital communications network to the secure computer of a ticket seller, a method for selling and for delivering a digital ticket from a ticket seller to a ticket buyer, the method comprising:

at a first time first-sending from the computer of the ticket seller across the communications network to the computer of the ticket buyer first data regarding events for which tickets may be had; then at a second time

second-sending from the computer of the ticket buyer across the communications network to the computer of the ticket seller second data identifying and event for which a ticket is desired, the second data accompanied by a secure first transformation of a number that is determined by the ticket buyer only and unknown to others including the ticket seller; then at a third time

third-sending from the computer of the ticket seller across the communications network to the computer of the ticket buyer third data confirming ticketing to the event

for which the ticket was desired, the third data accompanied by a secure second transformation of the secure first transformation; and then

storing, with the computer of the ticket buyer within a tangible portable medium of digital data storage, (i) the number in accompaniment to (ii) the secure second transformation;

wherein upon (i) transportation of the digital data storage medium to a physical site of the event, (ii) reading of the number to a computer, and, by use of the same secure first transformation that the buyer did use, reproduction of the secure first transformation of the number all over again, plus (iii) reversing of the secure second transformation by an event computer privileged to knowledge of said second transformation, then a (ii) read and reproduced first transformation is comparable to a (iii) first transformation recovered from reversing the second transformation in order to assess validity of the digital ticket;

wherein the communication channel is sending at the second time a random number.

2. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 25, 30-32, 39 and 46-48 have been cancelled.

5. Claims 1, 2, 34, 38, 45, 49 and 50-51 have been amended by Examiner's amendment.

6. Claims 1-24, 26-29, 33-38, 40-45 and 49-55 and , now re-numbered as claims 1-47 are pending.

Response to Arguments

7. Applicant's arguments filed 01/19/2006 have been fully considered and they are persuasive in the light of the agreement reached on the interview conducted on 02/06/2006 (see enclosed interview summary).

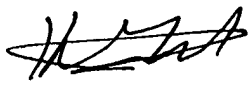
Allowable Subject Matter

8. Claims 1-24, 26-29, 33-38, 40-45 and 49-55 are allowed.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is 571-272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as 571-272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Kambiz Zand

02/07/2006

AU 2132